

# CoronaVirus

---

 [id-ransomware.blogspot.com/2020/03/coronavirus-ransomware.html](https://id-ransomware.blogspot.com/2020/03/coronavirus-ransomware.html)



## CoronaVirus Ransomware

---

## CoronaVirus Cover-Ransomware

---

(шифровальщик-вымогатель, MBR-модификатор)

---

(первоисточник на русском)

---

## Translation into English

---

Этот крипто-вымогатель шифрует данные пользователей с помощью AES, а затем требует выкуп 0.008 - 0.05 # BTC, чтобы вернуть файлы. Оригинальное название: CoronaVirus (указано в записке и текстах на экране). На файла может быть написано: WSHSetup.exe, Comparevalidatorlgamerefreshable.exe, sar.exe и прочее.

---

### **Обнаружения для Installer:**

**DrWeb** -> Trojan.Encoder.31254

**BitDefender** -> Trojan.GenericKD.33533697, Trojan.GenericKD.42839733

**ALYac** -> Trojan.Agent.Zenpak

**Avira (no cloud)** -> TR/Zenpak.rujhy

**ESET-NOD32** -> A Variant Of Win32/Kryptik.HBWA

**Fortinet** -> W32/Zenpak.HBWA!tr.ransom

**Kaspersky** -> Trojan.Win32.Zenpak.wqf

**Qihoo-360** -> Win32/Trojan.c84

**Rising** -> Trojan.Kryptik!8.8 (CLOUD)

**Symantec** -> Trojan Horse

**Tencent** -> Win32.Trojan.Zenpak.Syhv

---

### **Обнаружения для Ransomware:**

**DrWeb** -> Trojan.Encoder.31251

**BitDefender** -> Trojan.GenericKD.33538863, Generic.Ransom.Corona.C6172AAD

**ALYac** -> Trojan.Ransom.MBRlock

**Avira (no cloud)** -> TR/Ransom.MBRlock.nwhir, TR/ATRAPS.Gen5

**ESET-NOD32** -> A Variant Of Win32/MBRlock.AR

**Fortinet** -> W32/Upatre.AR!tr.dldr

**Kaspersky** -> Trojan-Downloader.Win32.Upatre.imly, Trojan-Downloader.Win32.Upatre.imoc

**Malwarebytes** -> Ransom.CoronaVirus

**Microsoft** -> Ransom:Win32/Filecoder.PF!MTB

**Qihoo-360** -> Win32/Trojan.Downloader.f9c, Win32/Trojan.Downloader.c98

**Rising** -> Trojan.Ransom.Satan.e (CLOUD), Trojan.Ransom.Satan.e (CLASSIC)

**Symantec** -> Trojan.Gen.MBT, Ransom.Gen, Ransom.Cryptolocker

**Tencent** -> Win32.Trojan-downloader.Upatre.Alsb, Malware.Win32.Gencirc.1134ca07

**TrendMicro** -> Ransom.Win32.MBRLOCK.AA, Ransom.Win32.KOROWNA.THCACBO

---

### **Обнаружения для файла трояна Крот:**

**DrWeb** -> Trojan.PWS.Steam.17860

**ALYac** -> Trojan.Stealer.Kpot

**Avira (no cloud)** -> TR/AD.Khalesi.wmfdt

**BitDefender** -> Trojan.GenericKD.33533023

**ESET-NOD32** -> A Variant Of Win32/Kryptik.HBVI

**Fortinet** -> W32/Kryptik.HBVI!tr

**Kaspersky** -> Trojan.Win32.Zenpak.wsd

**Malwarebytes** -> Trojan.Dropper

**Rising** -> Trojan.Kryptik!8.8 (CLOUD)

**Symantec** -> Trojan Horse

**Tencent** -> Win32.Trojan.Zenpak.Hupk

---

© Генеалогия: **Satana Ransomware + unknown** >> **CoronaVirus Ransomware**

**Родство подтверждено сервисом IntezerAnalyzer** >>

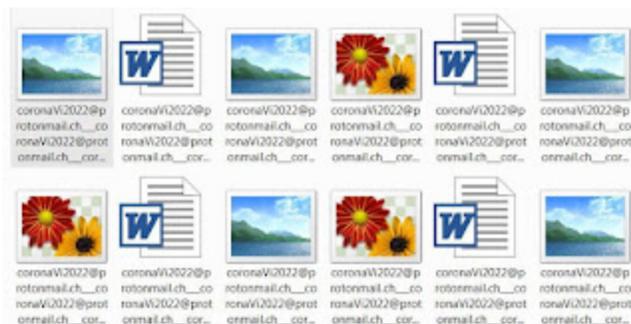


Изображение — логотип статьи

К зашифрованным файлам добавляется не расширение, а приставка: **coronavi2022@protonmail.ch\_\_**

Примеры зашифрованных файлов:

coronavi2022@protonmail.ch\_\_support.txt  
coronavi2022@protonmail.ch\_\_bugreport.html  
coronavi2022@protonmail.ch\_\_techinfo.rtf



### Этимология названия и пояснения:

Создатели распространители решили сыграть на громком названии вирусной эпидемии **COVID-19** (аббревиатура от англ. **CO**rona **VI**rus **D**isease 2019), сокращенно **CoronaVirus**, и добавили это слово в свои вымогательские тексты.

**Cover-Ransomware** — я ввел новое название для программ-вымогателей, которые являются прикрытием для установки других вредоносных программ. Ранее вымогатели или фейк-вымогатели, которые вели себя подобным образом, уже были описаны в нашем Дайджесте, но мы не выделяли это в отдельный вид.

В различных Cover-Ransomware вредоносным компонентом могут быть трояны различного действия, банковские трояны (банкеры), инфостилеры, стиратели, деструкторы, doxware, майнеры и прочие. Описание смотрите в нашем **Глоссарии**.



**Внимание!** Новые расширения, email и тексты о выкупе можно найти в конце статьи, в обновлениях. Там могут быть различия с первоначальным вариантом.

Активность этого крипто-вымогателя пришла на начало марта 2020 г. Ориентирован на англоязычных пользователей, что не мешает распространять его по всему миру.

Записка с требованием выкупа называется: **CoronaVirus.txt**



### **Содержание записки о выкупе:**

CORONAVIRUS is there

All your file are crypted.

Your computer is temporarily blocked on several levels.

Applying strong military secret encryption algorithm.

To assist in decrypting your files, you must do the following:

1. Pay 0.008 btc to Bitcoin wallet bc1q3v6far85gtdsrk4zu4fuhphheyqprwmuv62n92 or purchase the receipt Bitcoin;

2. Contact us by e-mail: coronaVi2022@protonmail.ch and tell us this your unique ID: D138101D44FEE2EB88495A67EEED1E89 and send the link to Bitcoin transaction generated or Bitcoin check number.

After all this, you get in your email the following:

1. Instructions and software to unlock your computer

2. Program - decryptor of your files.

Donations to the US presidential elections are accepted around the clock.

Desine sperare qui hic intras! [Wait to payment timeout 25 - 40 min]

### **Перевод записки на русский язык:**

КОРОНАВИРУС здесь

Все ваши файлы зашифрованы.

Ваш компьютер временно заблокирован на нескольких уровнях.

Применен сильный военный секретный алгоритм шифрования.

Для расшифровки ваших файлов вы должны сделать следующее:

1. Оплатить 0.008 btc на биткойн-кошелек

bc1q3v6far85gtdsrk4zu4fuhphheyqprwmuv62n92 или купить биткойны чеком;

2. Написать нам на email: coronaVi2022@protonmail.ch и сообщить нам свой уникальный ID: D138101D44FEE2EB88495A67EEED1E89

и отправить ссылку на сгенерированную биткойн-транзакцию или номер биткойн-чека.

После всего этого вы получите в своем письме следующее:

1. Инструкции и программу для разблокировки компьютера
2. Программа - дешифровщик ваших файлов.

Пожертвования на выборы президента США принимаются круглосуточно.

Desine sperare qui hic intras! [Подождите окончания платежа 25 - 40 минут]

Запиской с требованием выкупа также выступают тексты на экране, которые появляются после перезагрузки системы:

```
COBONAVIRUS is there
All your file are crypted.
Your computer is temporarily blocked on several levels.
Applying strong military secret encryption algorithm.

To assist in decrypting your files, you must do the following:
1. Pay 0.000 btc to Bitcoin wallet bc1q0w7kuj60dts3u70qak79a5eet5a76res5u
or purchase the receipt Bitcoin:
2. Contact us by e-mail: coronav12022@protonmail.ch and tell us this your
unique ID: B0067076A704D0302151F790AEB1008E
and send the link to Bitcoin transaction generated or Bitcoin check number.
After all this, you get in your email the following:
1. Instructions and software to unlock your computer
2. Program - decryptor of your files.
Donations to the US presidential elections are accepted around the clock.
Desine sperare qui hic intras! [Wait to payment timeout 25 - 40 min]
```

```
!!!!COBONAVIRUS is there!!!!
All your file are crypted.
Your computer is temporarily blocked on several levels.
Applying strong military secret encryption algorithm.

To assist in decrypting your files, you must
Pay to bitcoin wallet: bc1qkk6nmhsxvtp2akunhke3tjcy2w22kk00xa3jcontact us
via e-mail: coronav12022@protonmail.ch
Donations to the US presidential elections are accepted around the clock.
Desine sperare qui hic intras! [wait timeout 25 min]
```

Текст обоих примерно соответствует тексту из записки, с небольшими отличиями. Подробности в следующем разделе статьи.

## Технические детали

Может распространяться путём взлома через незащищенную конфигурацию RDP, с помощью email-спама и вредоносных вложений, обманных загрузок, ботнетов, эксплойтов, вредоносной рекламы, веб-инъектов, фальшивых обновлений, перепакованных и заражённых инсталляторов. См. также "Основные способы распространения криптовымогателей" на [вводной странице блога](#).

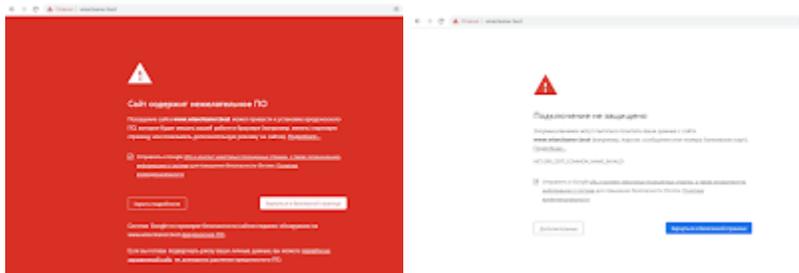
Для автоматического распространения вредоносного ПО злоумышленники создали веб-сайт [www.wisecleaner.best](http://www.wisecleaner.best), который внешне является копией официального сайта известной безопасной программы для восстановления данных Wise Data Recovery

(www.wisecleaner.com). На момент проверки сайта загрузки на этом сайте неактивны, но ранее с него распространялся файл WSHSetup.exe, который выполняет функцию загрузчика для CoronaVirus Ransomware и трояна-инфостилера Krot.

WSHSetup.exe после запуска пытается загрузить 7 файлов с сайта trynda.xyz (во время проверки смогли загрузиться только два файла file1.exe и file2.exe), затем устанавливает файл шифровальщика и **троян Krot**. Предназначение остальных файлов неизвестно.

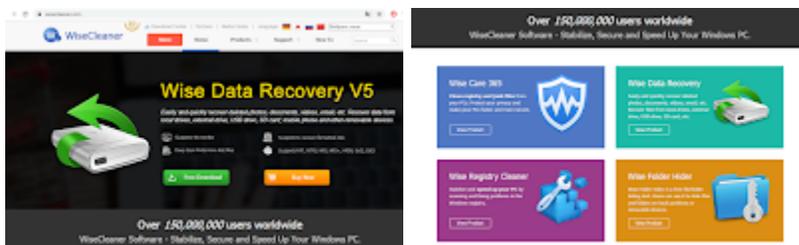
```
0 1 200 HTTP trynda.xyz /file.exe 735... applica... wshsetup-6644
0 2 200 HTTP trynda.xyz /file.exe 445... applica... wshsetup-6644
0 3 404 HTTP trynda.xyz /file.exe 178 text/html wshsetup-6644
0 4 404 HTTP trynda.xyz /file.exe 178 text/html wshsetup-6644
0 5 404 HTTP trynda.xyz /file.exe 178 text/html wshsetup-6644
0 6 404 HTTP trynda.xyz /file.exe 178 text/html wshsetup-6644
0 7 404 HTTP trynda.xyz /file.exe 178 text/html wshsetup-6644
0 8 200 HTTP Tunnel to blogger.org-443 0 wshsetup-6644
0 9 200 HTTPS google.g... /img/37 116 no-gl... #img/37 wshsetup-6644 Network ...
```

Во время нашей проверки сайт злоумышленников ещё был активен и система Google по проверке безопасности сайтов сообщила, что недавно на сайте на www.wisecleaner.best было обнаружено вредоносное ПО.



Поэтому, если вы используете настоящий браузер Google Chrome, а не одну из подделок и клонов, то у вас при открытии этого сайта должно появиться такое предупреждение. Официальный браузер Google Chrome можно скачать **по этой ссылке**.

Официальный сайт программы для восстановления данных Wise Data Recovery (https://www.wisecleaner.com) выглядит следующим образом:



Нужно всегда использовать Актуальную антивирусную защиту!!!

Если вы пренебрегаете комплексной антивирусной защитой класса Internet Security или Total Security, то хотя бы делайте резервное копирование важных файлов по методу 3-2-1.

➤ По мнению исследователей, CoronaVirus Ransomware используется в качестве прикрытия (англ. cover) для распространения инфекции трояна Krot, а не для получения выкупных платежей. Поэтому сумма выкупа довольно невелика по сравнению с другими вымогателям.

Таким образом, в данном случае основным вредоносом является **троян Krot**, предназначенный для кражи различной личной информации, включая учетные данные из установленных приложений и браузеров, игровых клиентов, почты и других служб, включая кошельки электронных платежных систем и хранения криптовалюты. Украденная информация отправляется на сайт злоумышленников.

➤ Пытается удалить теньные копии файлов, используя команды:

```
Delete Shadows /All /Quiet
```

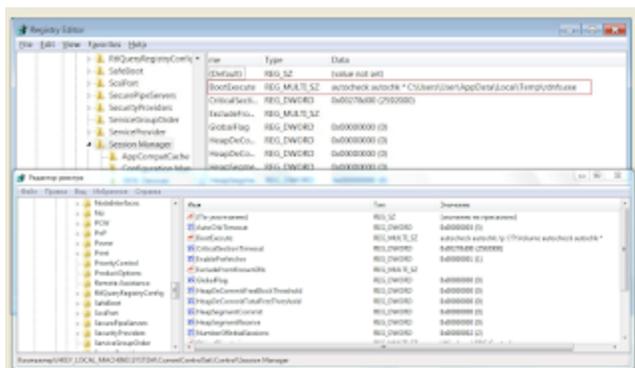
```
delete backup -keepVersions:0 -quiet
```

```
delete systemstatebackup -keepVersions:0 -quiet
```

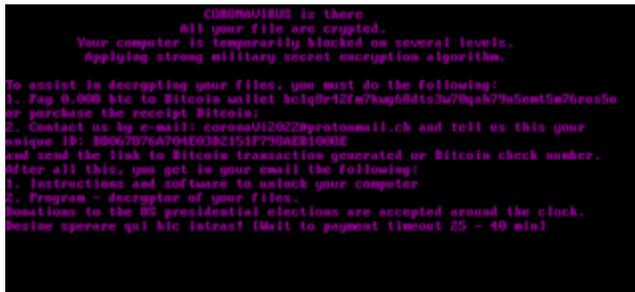
➤ Добавляется в Автозагрузку Windows.

➤ Перезаписывает MBR жесткого диска.

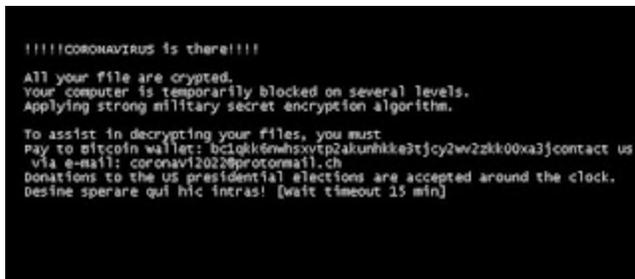
➤ Изменяет значение двоичного параметра "BootExecute" в разделе реестра HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager с используемого по умолчанию на "autocheck autochk \* C:\Users\User\AppData\Local\Temp\rdnfs.exe"



Эта операция позволяет запускать исполняемый файл из папки %Temp% перед загрузкой каких-либо служб Windows при запуске системы, чтобы показать жертве экран блокировки с уже знакомым текстом (гламурный цвет букв на чёрном фоне).



Примечательно, что через 45 минут экран блокировки переключится на немного другое сообщение (белые буквы на чёрном фоне). Здесь также отключена возможность выполнить ввести какие-либо действия или ввести какой-либо код, чтобы вернуться в систему.



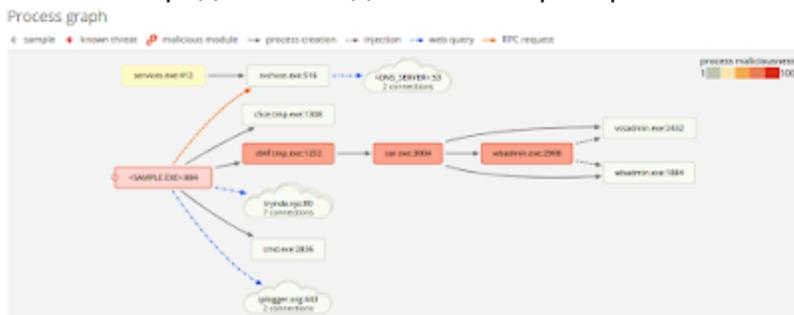
И это еще не все "прелести" этого вымогателя. Через 15 минут он загружается обратно в Windows и при входе в систему отображает записку с требованием выкупа — теперь уже файл CoronaVirus.txt.



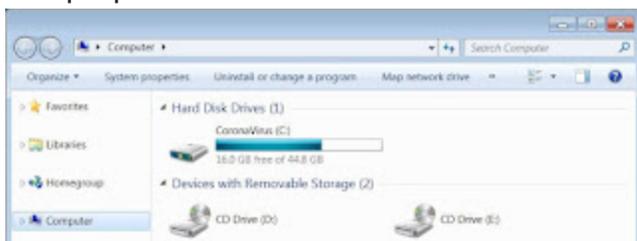
**🛑 Стоп!** Если вы дочитали статью до этого места, то вы должны немедленно с другого ПК или мобильного устройства зайти в свои аккаунты и сменить пароли на более сложные. Не забывайте, что троян Крот уже украл всё, что было на скомпрометированном ПК.

**Другие подробности**

► Схема вредоносных действий из рапорта Dr.Web vxCube:



► Программа-вымогатель изменяет название системного диска в "CoronaVirus".



Такое поведение мы видим впервые, за все время вымогательских атак с использованием Ransomware и шифрования.

**Список файловых расширений, подвергающихся шифрованию:**

.acc, .asm, .avi, .bak, .bat, .bmp, .cfu, .cpp, .cry, .csv, .dbf, .dgn, .doc, .dwg, .dxf, .epf, .erf, .gbr, .gho, .gif, .jpe, .jpg, .lic, .mdb, .mdf, .mht, .mov, .mxl, .ods, .odt, .old, .pas, .pdf, .png, .ppt, .rar, .rtf, .sdf, .stl, .tax, .tex, .tif, .txt, .vbs, .vpd, .vsd, .xls, .xml, .zip (49 расширений).

Это документы MS Office, OpenOffice, PDF, текстовые файлы, фотографии, видео, файлы образов, резервных копий, архивы, файлы лицензий, специальные файлы некоторых прикладных программ и игр.

**Файлы, связанные с этим Ransomware:**

CoronaVirus.txt - название текстового файла

WSSetup.exe - файл-загрузчик CoronaVirus Ransomware

file1.exe - файл трояна Krot

file2.exe - файл шифровальщика

<random>.exe - случайное название вредоносного файла, в рассматриваемом примере это файлы: hfyu.exe, sar.exe, c5ce.tmp.exe и прочие.

**Расположения:**

\Desktop\ ->

\User\_folders\ ->

\%TEMP%\ ->

%TEMP%\hfyu.exe

%TEMP%\sar.exe  
%TEMP%\qjpg.exe  
%APPDATA%\c5ce.tmp.exe  
%APPDATA%\c84f.tmp.exe  
C:\Users\User\AppData\Local\Temp\rdnfs.exe

### Записи реестра, связанные с этим Ransomware:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager  
"BootExecute"

См. ниже результаты анализов.

### Сетевые подключения и связи:

Файльшивый сайт: [www.wisecleaner.best](http://www.wisecleaner.best)

Malware URL: [xxxx://trynda.xyz/](http://xxxx://trynda.xyz/)

Malware URL + file Kpot: [xxxx://trynda.xyz/file1.exe](http://xxxx://trynda.xyz/file1.exe)

Malware URL + file CoronaVirus: [xxxx://trynda.xyz/file1.exe](http://xxxx://trynda.xyz/file1.exe)

Malware URL + files: [xxxx://trynda.xyz/{3}-{7}.exe](http://xxxx://trynda.xyz/{3}-{7}.exe)

The screenshot displays a VirusShare analysis interface with several sections:

- Network Communication:**
  - HTTP Requests:** A list of requests to <http://trynda.xyz/> with file names like file1.exe through file7.exe.
  - Contacted URLs:** A table showing scanned dates (2020-03-12), detection counts (e.g., 34 / 72), and URLs (e.g., <http://trynda.xyz/file2.exe>).
  - DNS Resolutions:** A list of domains like [trynda.xyz](http://trynda.xyz/) and [iplogger.org](http://iplogger.org/).
  - Contacted Domains:** A table showing domains, detection counts, creation dates, and registrars (e.g., REGTIME LTD).
  - IP Traffic:** Shows traffic to 88.99.66.31.443 (TCP).
  - Names:** Lists file names like [file1.exe](http://trynda.xyz/file1.exe) and [c5ce.tmp.exe](http://trynda.xyz/c5ce.tmp.exe).
- Signature Info:** Shows "File is not signed".
- Signature Verification:** Shows "File is not signed".
- File Version Information:** Provides metadata for files like [c5ce.tmp.exe](http://trynda.xyz/c5ce.tmp.exe) (Copyright © 2000-2014 KG and its Licenses-Crawler.com) and [file1.exe](http://trynda.xyz/file1.exe) (Copyright © DocuSign, All rights reserved).

Email: [coronaVi2022@protonmail.ch](mailto:coronaVi2022@protonmail.ch)

BTC: [bc1q8r42fm7kwg68dts3w70qah79n5emt5m76rus5u](https://bc1q8r42fm7kwg68dts3w70qah79n5emt5m76rus5u)

См. ниже в обновлениях другие адреса и контакты.

См. ниже результаты анализов.

### Скриноты кода и функций CoronaVirus (от исследователей):




---

=== ИСТОРИЯ СЕМЕЙСТВА === HISTORY OF FAMILY ===

---

=== БЛОК ОБНОВЛЕНИЙ === BLOCK OF UPDATES ===

---

=== БЛОК ССЫЛОК и СПАСИБОК = BLOCK OF LINKS AND THANKS ===



Thanks:

MalwareHunterTeam, Michael Gillespie, Vitali Kremez  
 Andrew Ivanov (author),  
 Lawrence Abrams, dnwls0719  
 to the victims who sent the samples

© Amigo-A (Andrew Ivanov): All blog articles. [Contact](#).